**91.460-530.203 Cyber Crime Investigation**

**Term Project**

**(20 points towards the final grade)**

### Instructions:

1. Note: Blue text points to a web link. Ctrl + Click to follow link.
2. This is an individual assignment.
3. Answers to all questions including hands-on project with screen shots must be put into **ONE** document. That is, every time, each student can only submit one report document, answering all questions of this assignment.
4. Students must put answers following each question in this assignment. The instructor will not grade a report with only answers in it and the student gets zero for such an assignment. An assignment report must include original questions.
5. Students MUST submit the finished assignment in either Microsoft Word or pdf format to Blackboard. The doc must be submitted as a standalone file and cannot be tarred or zipped into a container.
6. All Hands-on exercise that operates some software is required with screenshots of the actions to prove that the project is performed. The required screenshots must be put into the doc at appropriate place with explanation.
7. Refer to [Print screen](http://en.wikipedia.org/wiki/Print_screen) on how to take a screenshot. Pressing the Alt key in combination with PrtSc will capture the currently selected window.
8. Please refer to the references at the end for hints.

* **Every student must submit the group report. Students get 0 for the project if the report is not submitted.**
* **Do not change the password of student on the gateway.**

**Project description**

* Please fill out the form at <https://docs.google.com/spreadsheets/d/1V24c9QqToGYlAXm1lZh2rf4ZsnmhcRRsHhuPqYNhsZg/edit?usp=sharing>. We can have at most 10 teams. The group number (X from 1 to 10) will be used later in the instruction.
* Here is the instruction to get into your virtual machines and VM assignment:

1. *ssh* ***your\_cs\_username****@mercury.cs.uml.edu* (Log into our cs server. If VPN is used or the student uses the campus network, skip this step)

2. *ssh -p 5300 student@cs.uml.edu* (Login into gateway. User name: student; Password: CyberCr1me)

3. *ssh root@Kali****X*** (Login the Kali VM. Change X to your group number, 1 to 10.)

and

ssh msfadmin@metasexploitX (Log into the Metasploitable2 VM. X is number 1 to 10)

Note: Account info

gateway - student/CyberCr1me

kali1-10 - root/kali

metasexploit1-10 - msfadmin/msfadmin

* **Editors**: ***vi*** [5] may be used at a Metasploitable2 VM. **nano** [6] may be used at a Kali VM. Input *export TERM=xterm* in the Metasploitable2 console to [correct the setting of](http://stackoverflow.com/questions/6804208/nano-error-error-opening-terminal-xterm-256color) *[nano](http://stackoverflow.com/questions/6804208/nano-error-error-opening-terminal-xterm-256color)* or add the command to *~/.bashrc* in order to use *nano* under the Metasploitable2 VM.
* Kali uses rsyslogd and Metasploitable2 VM uses syslogd.
* The configuration phase will end on midnight, Apr. 24, 2017, you should change your root password of VMs and remember it.
* The attack phase starts on Apr. 25 early morning and ends at 11:59PM on Apr. 30, 2017.
* Note: Do not change the password of *student* on the gateway.

### Requirements:

### Perform at least 5 different attacks in total against other groups, not yourself. One of the attacks must be through metasploit. (10 points)

### Detect attacks against your Kali and Metasploitable2 VMs. Lose one point for each undetected attack and lose at most 10 points. (10 points)

### A powerpoint presentation of attacks and detection by each group will be from 11:30AM - 2:30PM on 5/1/2017, Monday. The powerpoint presenation is the report students should submit to Blackboard.

1. Please refer to [1] about how to configure Kali and use metasploit.

### Please refer to [2][3][4] about Metasploitable 2.

### Note: a group cannot “shut down” their metasploitable VM to prevent attacks. This strategy does not make sense at all. If the group itself cannot log into their metasploitable VM, they lose 5 points.

### References

1. Metasploit Framework, <http://docs.kali.org/general-use/starting-metasploit-framework-in-kali>, 2017
2. Metasploitable 2 Exploitability Guide, https://community.rapid7.com/docs/DOC-1875, Dec 13, 2013
3. Metasploitable 2 enumeration, <http://www.hackingtutorials.org/metasploit-tutorials/metasploitable-2-enumeration/>, May 7, 2016
4. Metasploitable 2 vulnerability assessment, <http://www.hackingtutorials.org/metasploit-tutorials/metasploitable-2-vulnerability-assessment/>, June 5, 2016
5. Basic vi Commands, <https://www.cs.colostate.edu/helpdocs/vi.html>, 2017
6. Nano basics, <https://wiki.gentoo.org/wiki/Nano/Basics_Guide>, 2017
7. rsyslogd - reliable and extended syslogd, <http://man7.org/linux/man-pages/man8/rsyslogd.8.html>, 02 Dec 2014
8. sysklogd - Linux system logging utilities, <https://linux.die.net/man/8/syslogd>, 2017